Tecnologias de Redes de Comunicações

2006/2007

HFC

Fernando M. Silva

Fernando.Silva@ist.utl.pt

Instituto Superior Técnico

Sumário

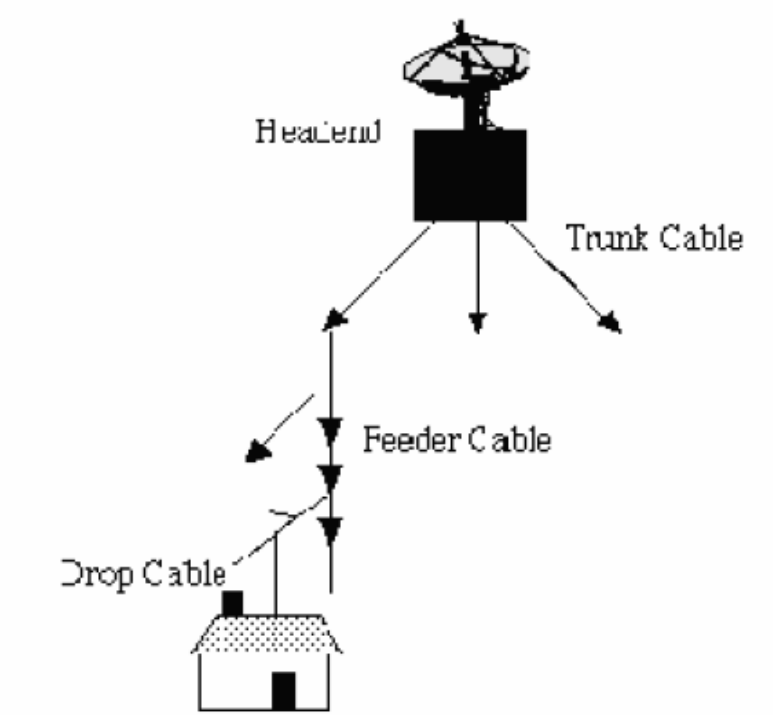
- HFC - *Hybrid Fiber Coax*
  - Redes Híbridas Fibra Cabo Coaxial
- Arquitectura
- Normas DOCSIS
- Protocolos
- Camada Física
- Camada MAC

Origem

- Redes analógicas
- Distribuição undirecional
- Rede totalmente em cabo coaxial
- Elevado número de repetidores/regeneradores de sinal
  - Podiam ser atingidos 30 a 40 amplificadores

Arquitectura Tradicional de Sistemas de TV por cabo

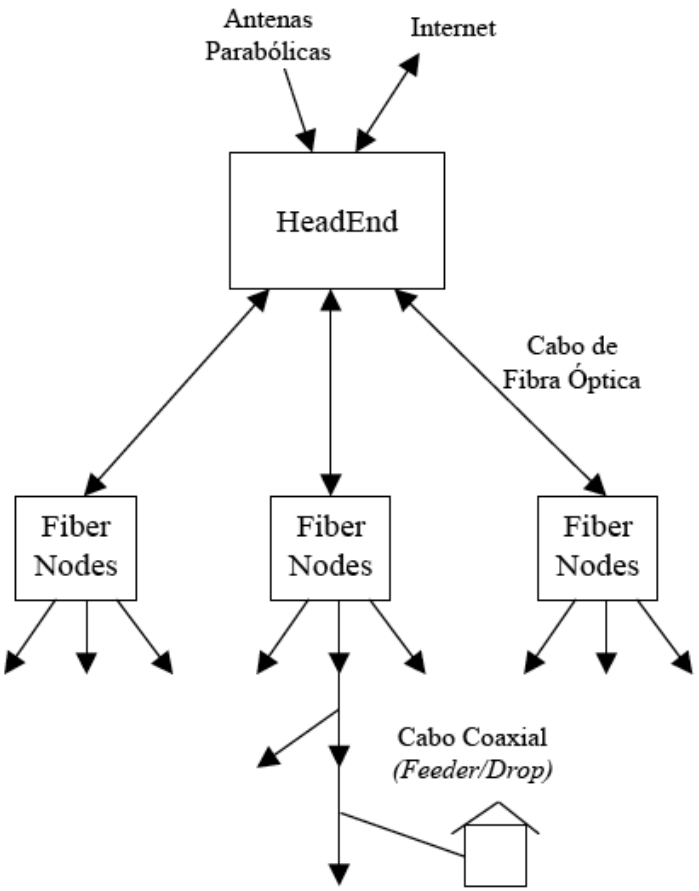
- Sub-rede primária (*Trunk cable*)- 10% da infraestrutura
- Sub-rede secundária (*Feeder cable*)- 40%
- Cabo de cliente *(Drop cable) - 50%*



Evolução para HFC

- Factores que ditaram a evolução do sistemas de cabo
  - Redução dos custos de implementação/manutenção
    - Substituição de grande parte do sistema de distribuição por Fibra Óptica (FO)
    - Manutenção do cabo apenas na fase terminal do sistema
    - Redução do número de amplificadores/regeneradores do sinal
  - Tecnologia de Vídeo Digital
    - Técnicas de compressão (MPEG1, MPEG2, MPEG4).
    - Técnicas de transmissão digital
    - Maior qualidade do sinal
    - Possibilidade de transmissão bidireccional
- Durante a década de 90, assistiu-se à progressiva substituição dos sistemas CATV analógicos por sistemas digitais híbrídos fibra/cobre
- A maioria da distribuição é realizada em fibra, restringindo-se o cabo coaxial ás zonas de distribuição.
  - Redes Híbridas HFC

Arquitectura HFC



Características HFC

- Células de dimensão variável
- Número máximo de amplificadores: 4 a 6
- Capacidade das células: 500 a 2000 domicílios

Capacidade vs largura de banda

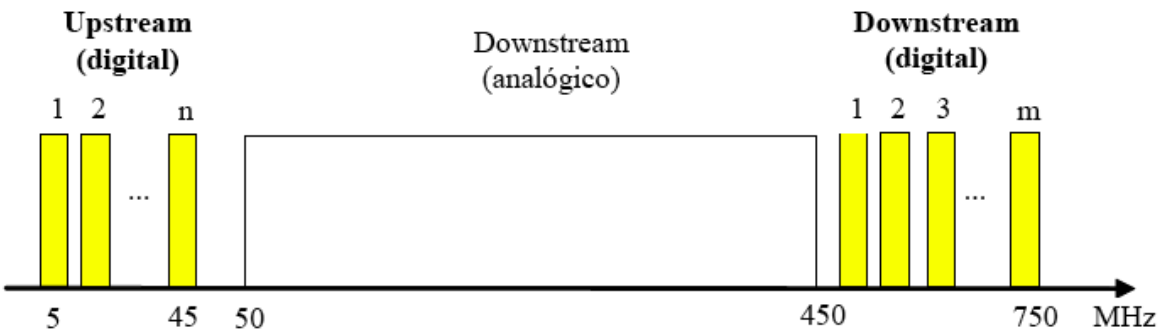
- Capacidade de canal: teorema Shannon?Hartley

  $C = B \log_2(1 + \frac{S}{N})$

  - B - Largura de banda em Hz
  - C - Capacidade em bits / segundo
- Problema: Como varia a capacidade do canal em funcão da relação sinal ruído, em dbs?
- Valores de referência
  - Canal analógico de televisão 7MHz
  - Codificação de vídeo: 3 a 6 Mbit/s
- Conclusões?

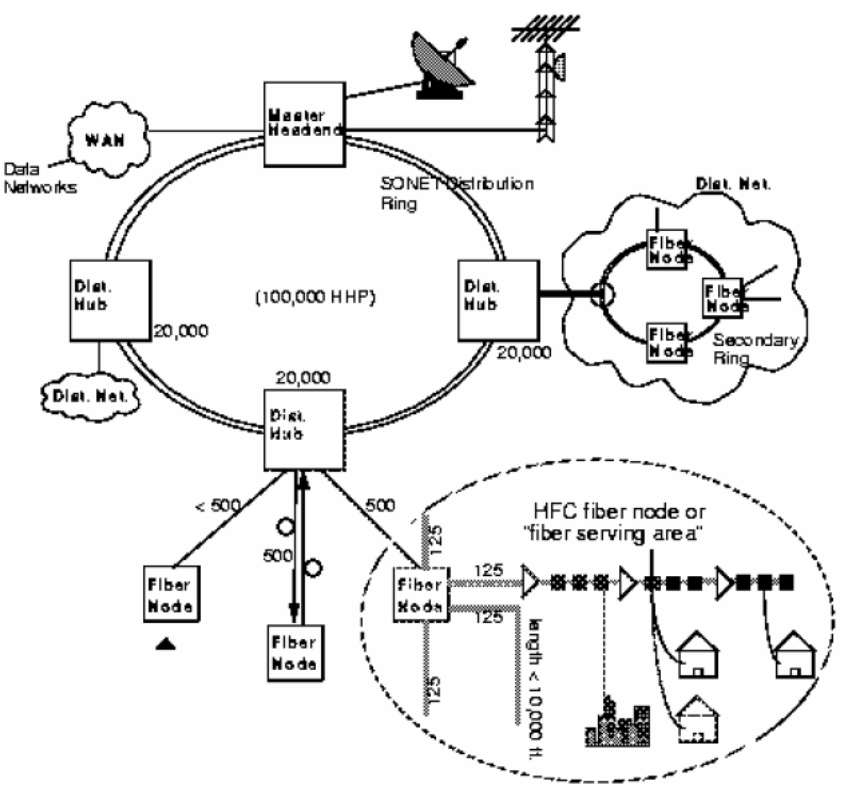
Serviços

- Tendência actual: serviço individualizado por cliente (por oposição a difusão simples)
- Técnicas que permitem atingier este objectivo
  - Aumento da largura de banda
  - Segmentação da rede/re-utilização do espectro
  - Compressão digital de vídeo



- Sentido ascendente - 5-40 Mhz: retorno digital
- Sentido descendente - 50-450Mhz: difusão analógico
- Sentido descendente - 450Mhz-750Mhz: digital
- Problemas
  - Acumulação de ruído, nos amplificadores de sinal, sobretudo presente no sentido ascendente

- Em países em que os operadores dispõeêm de redes de CATV dispersas geograficamente, existem redes regionais em fibra óptica de modo a interligar e integrar essas redes.



Normas

- Durante muito tempo, verificou-se a proliferação de soluções proprietárias para a distribuição em redes HFC
- Os requisitos de interoperabilidade e compatibilidade obrigaram a desenvolver normas.
  - *IEEE 802.14 working group*
    - Definiu a camada física e a camada de acesso ao meio para o transporte de dados
    - A arquitectura de referência especifica uma infra-estrutura de de FO/COAX com um raio de 80Km a partir da cabeça da rede
  - *MCNS - Multimedia Cable Network System Partners*
    - Associação de da maioria dos operadores de cabo da América do Norte
    - Patrocina uma instituição de investigação e desenvolvimento *CableLabs*
    - Objectivos da *CableLabs*:
      - Desenvolver especificações técnicas de interfaces
      - Permitir a compatibildidade entre fabricantes

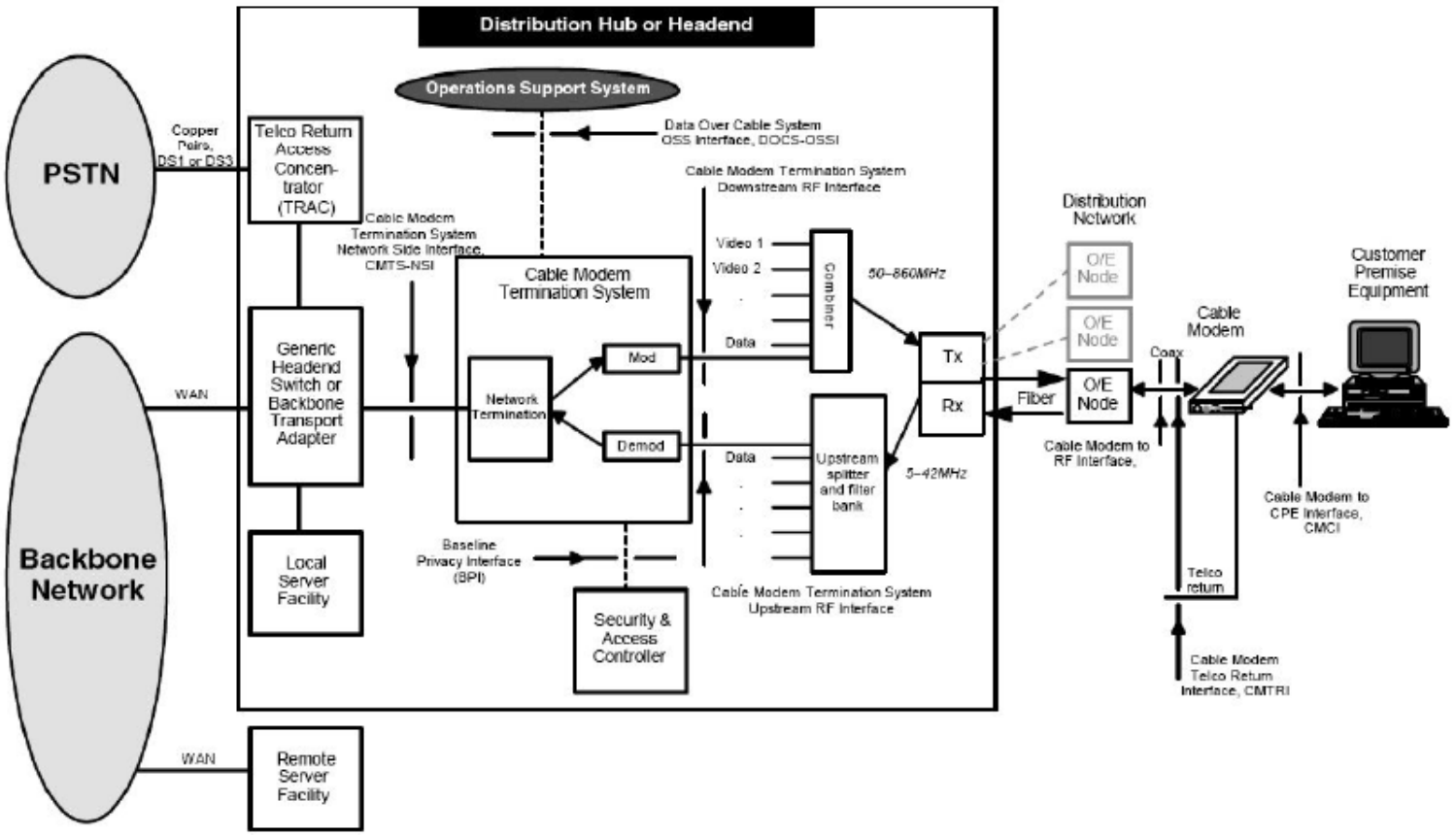
Normas DOCSIS

- Criação do IEEE802.14: 1994
- Criação do MCNS: 1996
  - Março de 1997: publicação do primeiro *draft* das especificações designado ***Data Over Cable Service Interface Specifications*** (DOCSIS 1.0)
  - Início de 1998: início da certificação formal de equipamentos
  - Março de 1998: ITU adopta o DOCSIS como norma ITU J.112
  - Abril 1999: DOCSIS 1.1 (suporte de QoS, capacidade de fragmentação de pacotes em h/w)
  - Dez 2004: DOCSIS 2.0

Evolução das normas DOCSIS

	Máx largura de banda por canal	Eficiência espectral/ modulação	Máx. Débito de Dados por canal
DOCSIS 1.0	3,2 MHz	1,6 bps/Hz (QPSK)	5,12 Mbps
DOCSIS 1.1	3,2 MHz	3,2 bps/Hz (16 QAM)	10,24 Mbps
DOCSIS 2.0	6,4 MHz	4,8 bps/Hz (64 QAM ou 128 QAM/TCM)	30,72 Mbps

Arquitectura de referência DOCSIS



Características

- Transmissão bidireccional
- Distância máxima de 160Km entre o CMTS (Cable Modem Termination System, Head end) e o Cable modem mais distante (distância padrão 16 a 20Km).
- Cada nó de fibra (célula) pode servir entre 500 a 2000 utilizadores, dependendo da largura de banda disponibilizada a cada um.

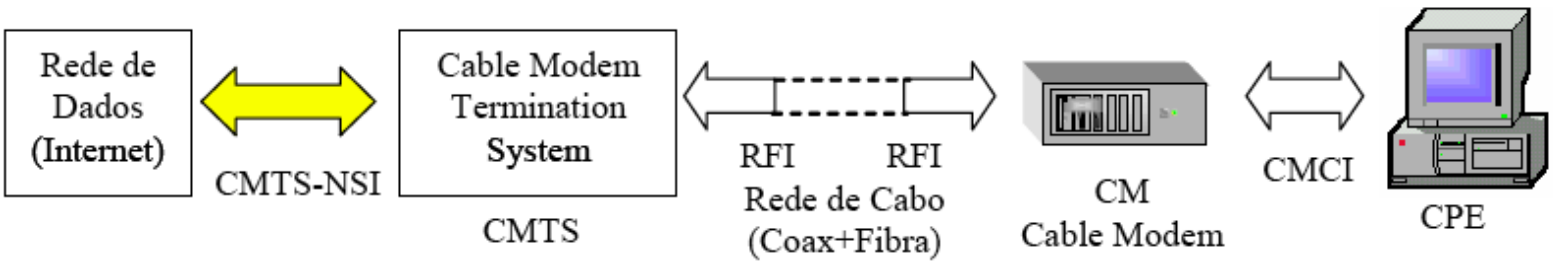
Estrutura das normas DOCSIS

- 11 documentos, disponíveis em DOCSIS 2.0
  - Interface de modem de cabo - CMCI
  - Interface de retorno telefónico - CMTRI
  - Interface rede-cabo CMTS-NSI
  - Interface de rádio RF
  - Interface de privacidade BRI (Baseline Privacy Interface)
  - Interface de Suporte de Operações - Interfaces de gestão entre os elementos da rede e de gestão de alto nível

- Portocolos considerados nas normas DOCSIS
  - Camada de rede (IP)
  - Camada de ligação de dados
    - Subcamada LLC (Logic Link Layer)
      norma IEEE 802.2
    - Subcamada de segurança
      Privacidade, autenticação e autorização
    - Subcamada MAC
      PDUs de comprimento variável
  - Camada física
    - Uptream/Downstream Transmission convergence
    - Physical Media Dependent

Protocolos na interface CMTS-NSI

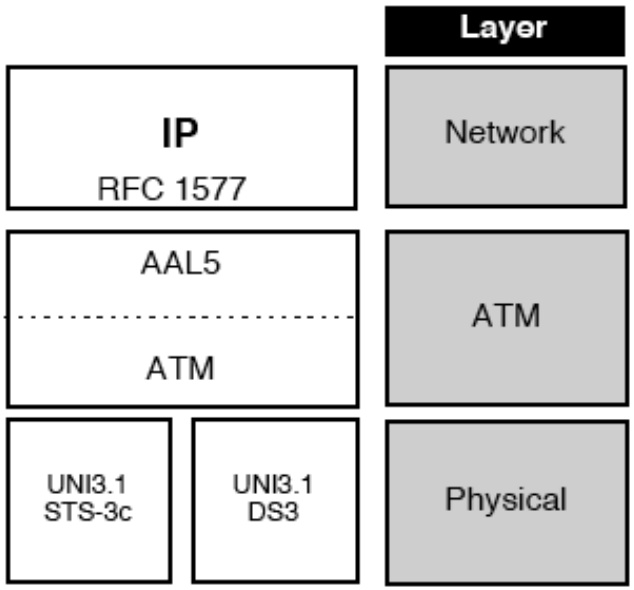
A interface CMTS-NSI (Cable Modem Termination System - Network System Interface) inclui um conjunto de especificações que se destinam a facilitar a implementação de serviços de dados sobre HFC.



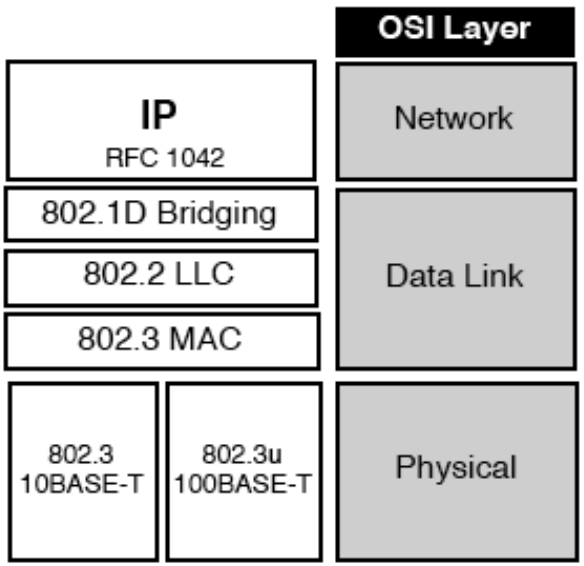
Interfaces

- São consideradas várias combinações possíveis de camadas físicas e de dados
- Pressuposto do protocolo IP na camada de rede
- Camadas de dados e físicas devem suportar e ser transparentes às normas utilizados
  - ATM sobre STS-3c (SONET)
  - ATM sobre DS3 (E3 44.3 Mbit/s)
  - FDDI (100Mbit/s)
  - 802.3 sobre 10Base-T e 100Base-T
  - Ethernet sobre 10Base-T e 100Base-T

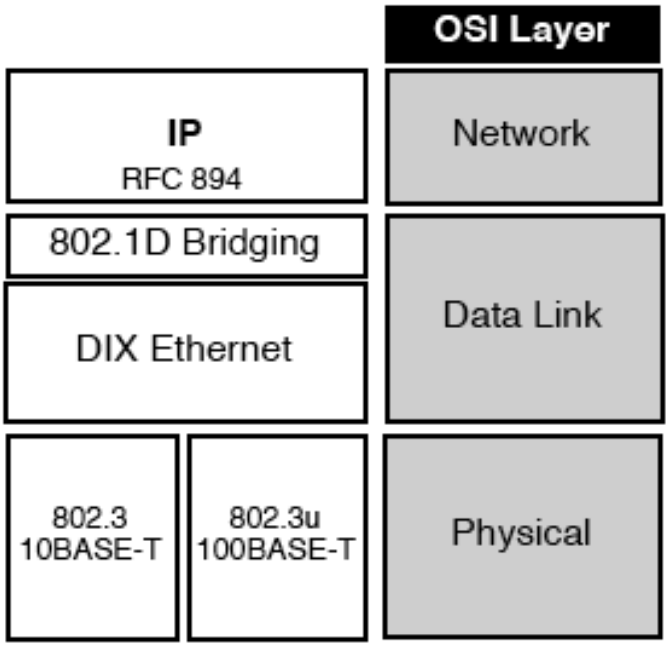
IP sobre ATM


Layer
IP
RFC 1577
Network
AAL5
ATM
ATM
UNI3.1
STS-3c
UNI3.1
DS3
Physical

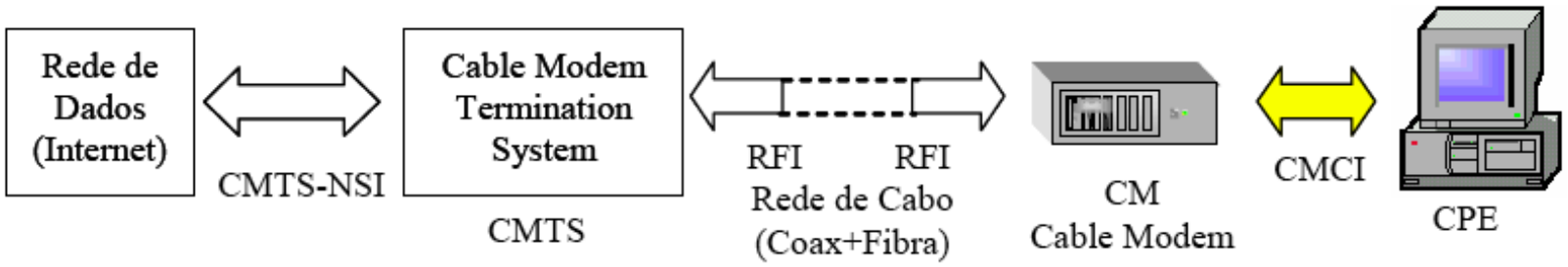
IP sobre 802.3



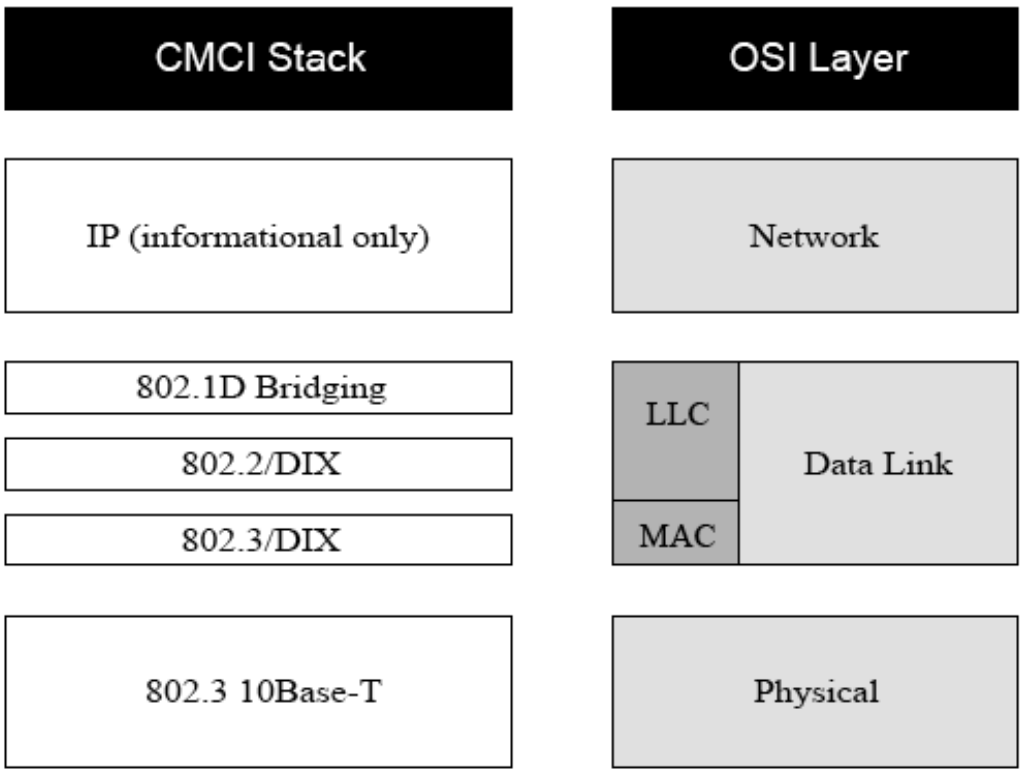
IP sobre Ethernet

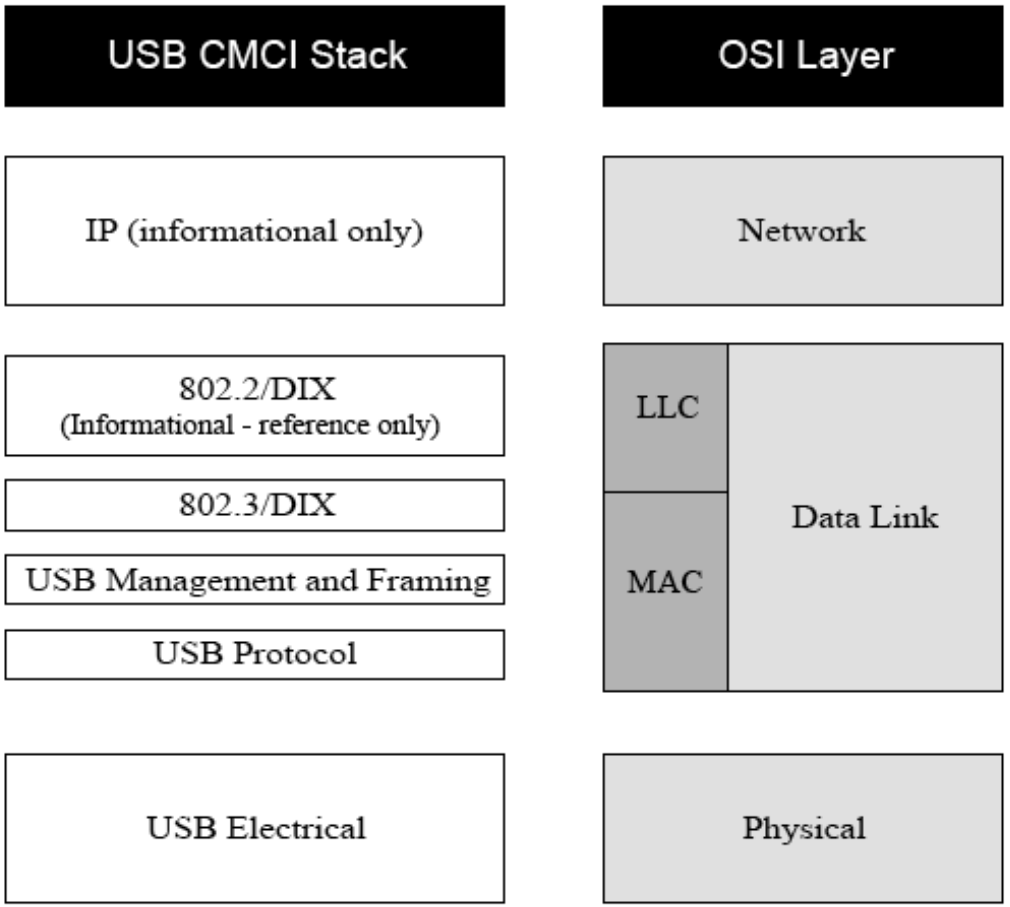


Protocolos na interface CMCI

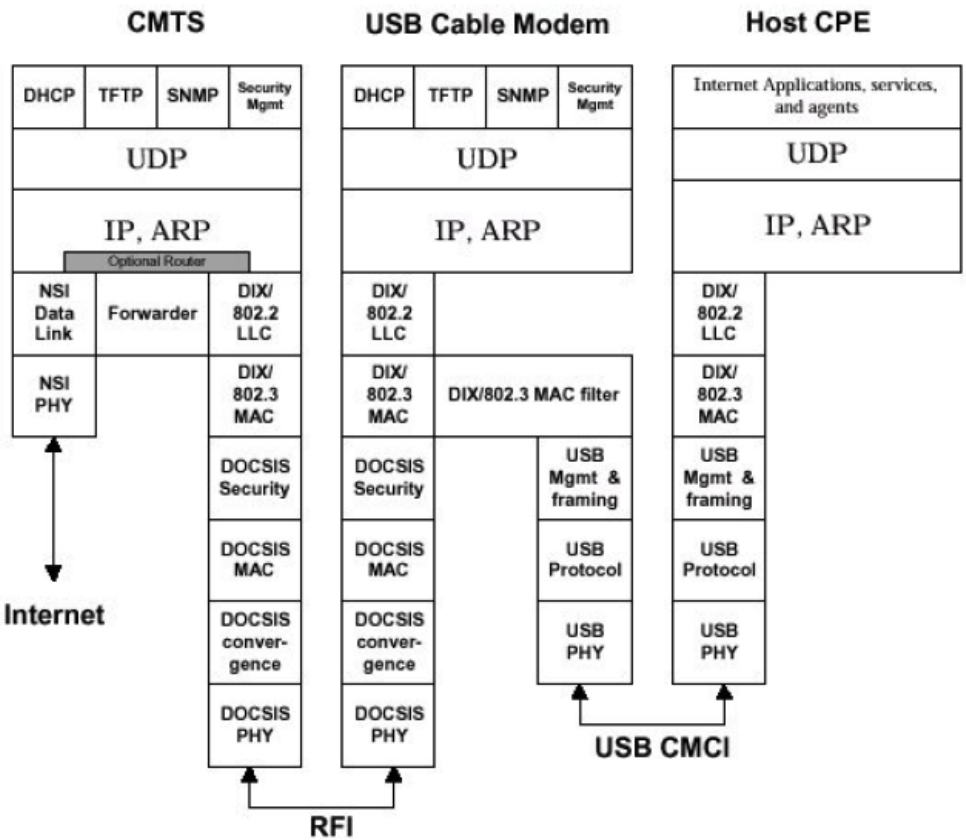


CMCI ethernet

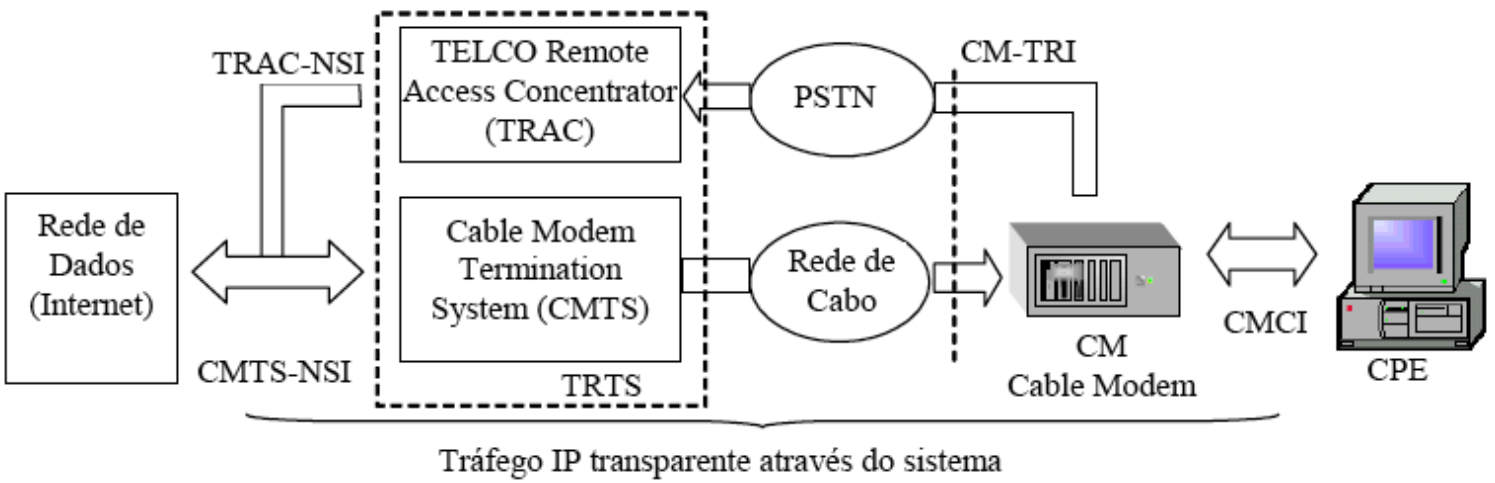



USB CMCI Stack
OSI Layer
IP (informational only)
Network
802.2/DIX
(Informational - reference only)
802.3/DIX
USB Management and Framing
USB Protocol
LLC
MAC
Data Link
USB Electrical
Physical

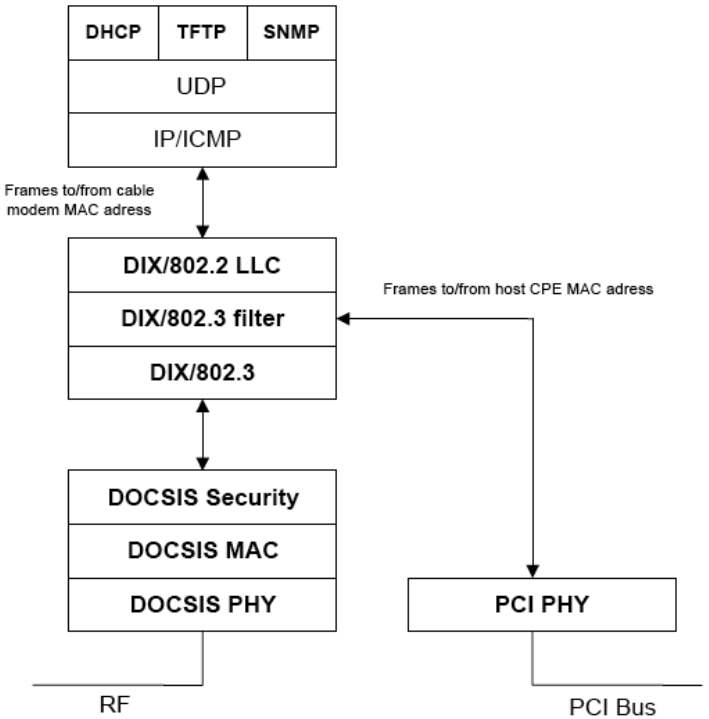
Pilha de protocolos HFC, CPE com USB



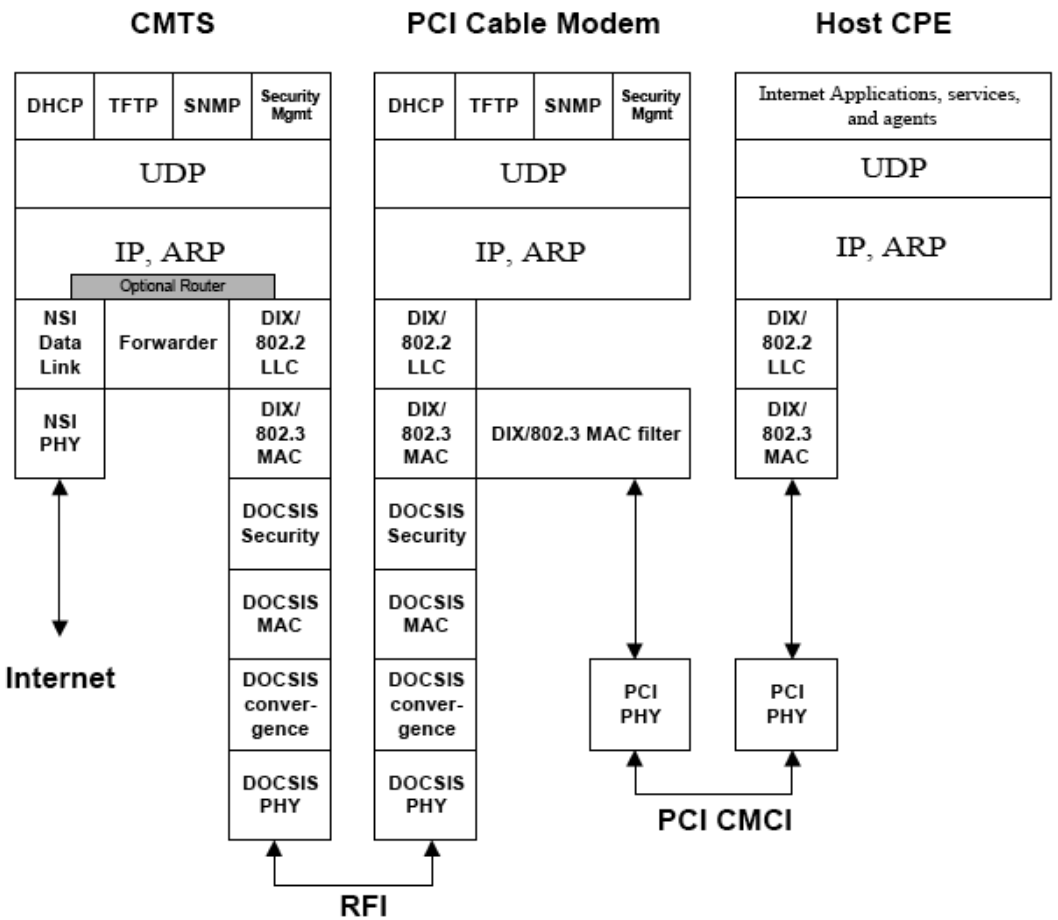
- No caso de não ser possível retorno pela rede, este pode ter lugar via PSTN
- Exige um TRAC (Telephone Remote Access Concentrator)
- CMTS e TRAC estão normalmente juntos no head end e são denominados Telephone Return Termination System (TRTS)



Pilha de protocolos - modem interno



Transporte de dados - Modem interno



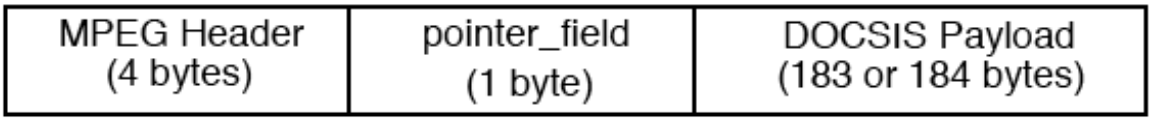
- Sentido descendente
  - Physical Media Dependent
    - Modulação 64QAM ou 256QAM
    - ritmos 5Msymbol/s=30Mbits/s,40Mbit/s
    - Frequência central 91-857MHz
  - Downstream Transmission Convergence
    - A camada *Downstream Transmission Convergence* fornece serviços de vídeo ou dados, sendo por isso baseada em baseada em pacotes MPEG de 188 bytes

- No sentido descendente baseia-se num stream contínuo de pacotes MPEG, com 188 bytes.
- O header do pacote MPEG indica se o pacote é vídeo ou se DOC (Data Over Cable)

header=DOC	DOC MAC payload
header=video	digital video payload
header=video	digital video payload
header=DOC	DOC MAC payload
header=video	digital video payload
header=DOC	DOC MAC payload
header=video	digital video payload
header=video	digital video payload
header=video	digital video payload

Formato do pacote MPEG

- O formato de um pacote mpeg com dados DOCSIS é o seguinte:



Formato do header pacote MPEG

- Estrutura do cabeçalho de um pacote MPEG

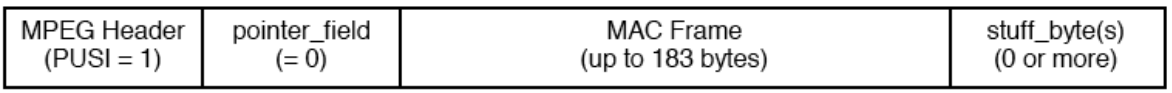
Field	Length (bits)	Description
sync_byte	8	0x47; MPEG Packet Sync byte
transport_error_indicator	1	Indicates an error has occurred in the reception of the packet. This bit is reset to zero by the sender, and set to one whenever an error occurs in transmission of the packet
payload_unit_start_indicator	1	A value of one indicates the presence of a pointer_field as the first byte of the payload (fifth byte of the packet)
transport_priority	1	Reserved; set to zero
PID	13	DOCSIS Data-Over-Cable well-known PID (0x1FFE)
transport_scrambling_control	2	Reserved, set to '00'
adaptation_field_control	2	'01'; use of the adaptation_field is NOT ALLOWED on the DOCSIS PID
continuity_counter	4	cyclic counter within this PID

Formato do header pacote MPEG

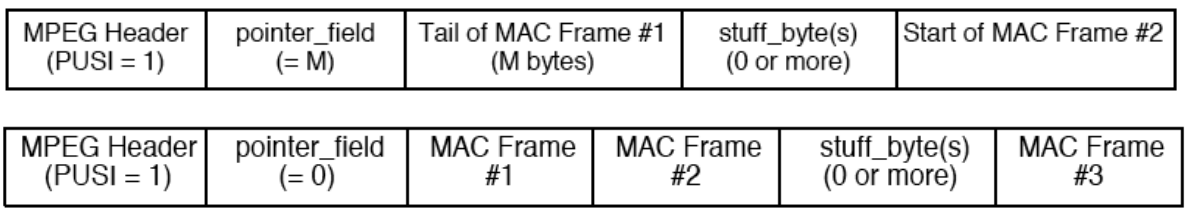
- Estrutura do cabeçalho de um pacote MPEG

Field	Length (bits)	Description
sync_byte	8	0x47; MPEG Packet Sync byte
transport_error_indicator	1	Indicates an error has occurred in the reception of the packet. This bit is reset to zero by the sender, and set to one whenever an error occurs in transmission of the packet
payload_unit_start_indicator	1	A value of one indicates the presence of a pointer_field as the first byte of the payload (fifth byte of the packet)
transport_priority	1	Reserved; set to zero
PID	13	DOCSIS Data-Over-Cable well-known PID (0x1FFE)
transport_scrambling_control	2	Reserved, set to '00'
adaptation_field_control	2	'01'; use of the adaptation_field is NOT ALLOWED on the DOCSIS PID
continuity_counter	4	cyclic counter within this PID

- Os pacote MPEG com uma trama MAC contêm um campo adicional "Field Pointer" que indica quantos bytes é necessário saltar até ao início da próxima trama
- Quando uma trama MAC não preenche totalmente um pacote MPEG, o restante do pacote é preeenchido com *stuffing bytes* FF (valor nunca presente no cabeçalho de uma trama MAC)



- Na prática, um pacote MPEG pode conter um ou mais tramas MAC, ou uma trama MAC pode usar vários pacotes MPEG:



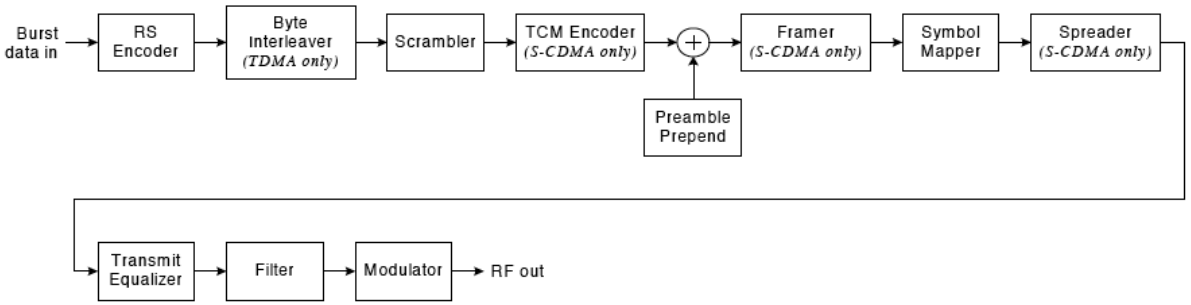
- Trama MAC pode usar vários pacotes MPEG:

MPEG Header (PUSI = 1)	pointer_field (= 0)	stuff_bytes (0 or more)	Start of MAC Frame #1 (up to 183 bytes)	
MPEG Header (PUSI = 0)	Continuation of MAC Frame #1 (184 bytes)			
MPEG Header (PUSI = 1)	pointer_field (= M)	Tail of MAC Frame #1 (M bytes)	stuff_byte(s) (0 or more)	Start of MAC Frame #2 (M bytes)

Camada física, upstream

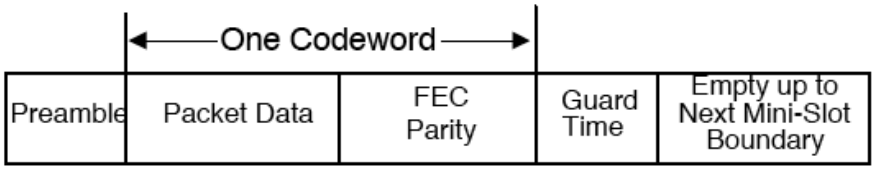
- Dois formatos suportados:
  - FDMA/TDMA - Divisão por frequência e slots temporais
  - FDMA/TDMA/S-CDMA - Vários modems podem operar no mesmo slot temporal e de frequência, sendo distinguidos por códigos ortogonais.
  - O modo específico de operação é definido pelo CMTS através de mensagens MAC enviadas ao CM
- Formatos de modulação
  - FDMA/TDMA - QPSK e 16QAM
  - S-CDMA e FDMA/TDMA - QPSK, 8QAM, 16QAM, 32QAM e 64QAM
  - S-CDMA deves suportar TCM (Trellis Code Modulation)

Sequência de processamento do sinal ascedente

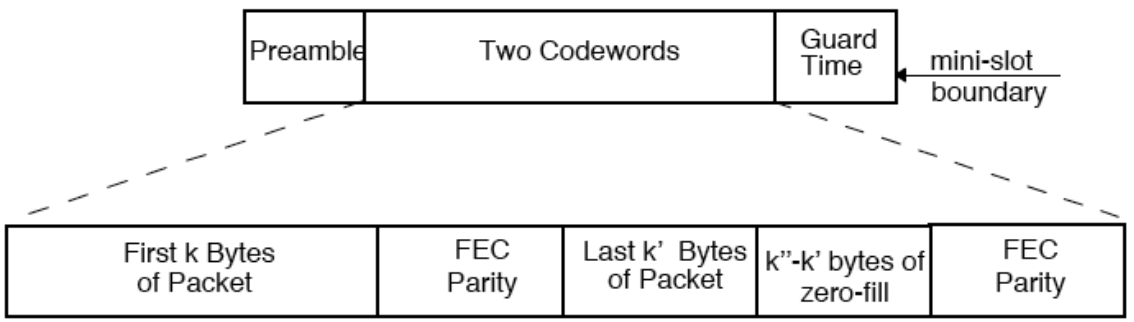


- Correcção de erros: código Reed-Solomon com T=1-16
- Valor de T programado pelo CTMS
- Tamanho mínimo de um pacote: 16 bytes, adicionados 0 se necessário

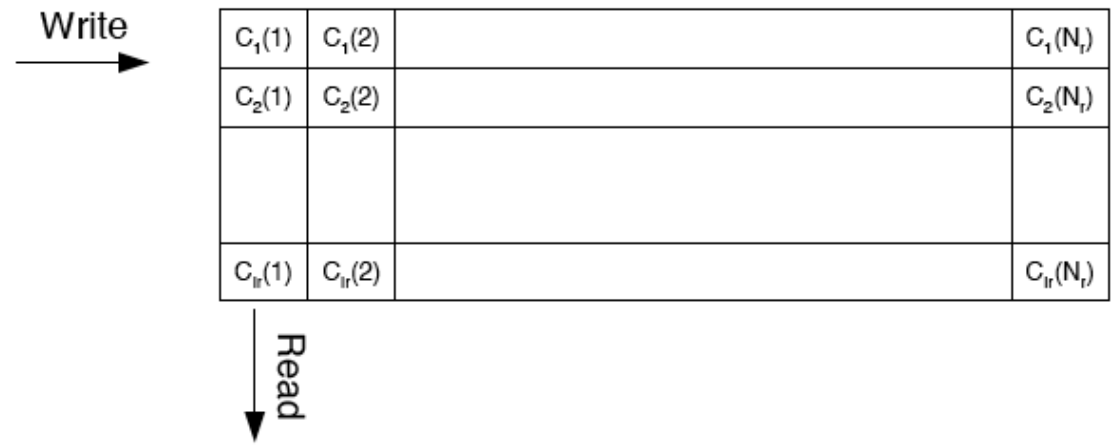
Example 1. Packet length = number of information bytes in codeword = k



Example 2. Packet length = k + remaining information bytes in 2nd codeword = k + k≤ k + k"



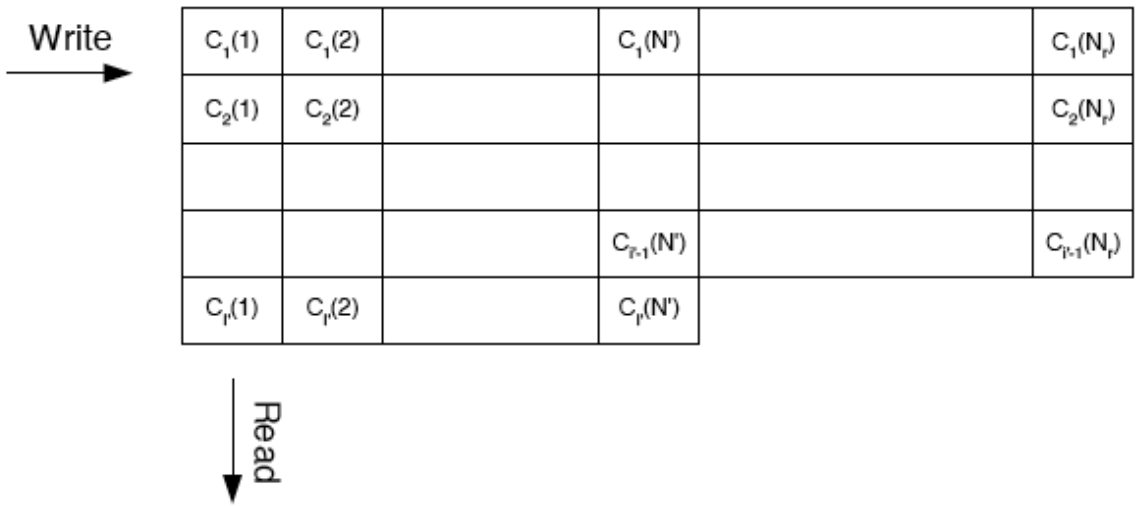
- O entreleçamento tem como objectivo reduzir efeitos de "bursts" de ruído, distribuindo os erros de uma única "codeword" do código RS por várias codewords.



Input sequence: $C_1(1),...C_1(N_r),C_2(1),....C_2(N_r),C_3(1).....C_{lr}(N_r)$

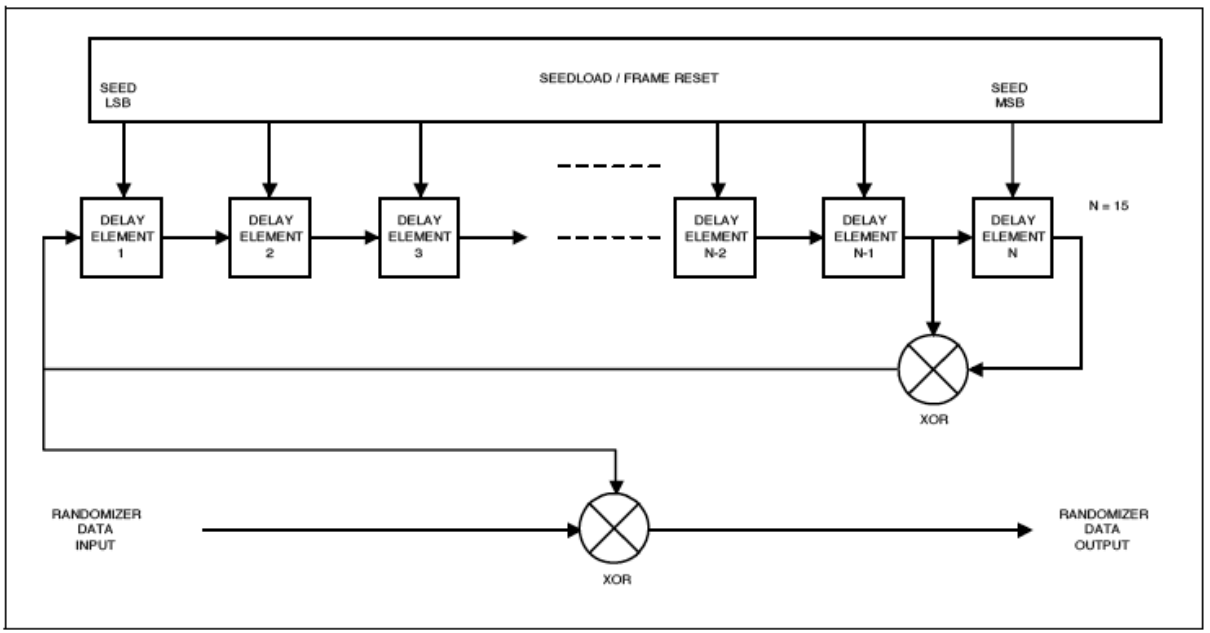
Output sequence: $C_1(1),C_2(1)...C_{lr}(1),C_1(2),....C_{lr}(2),C_1(3).....C_{lr}(N_r)$

- Modo fixo: O último subbloco pode ficar incompleto (em último caso, 1 byte)



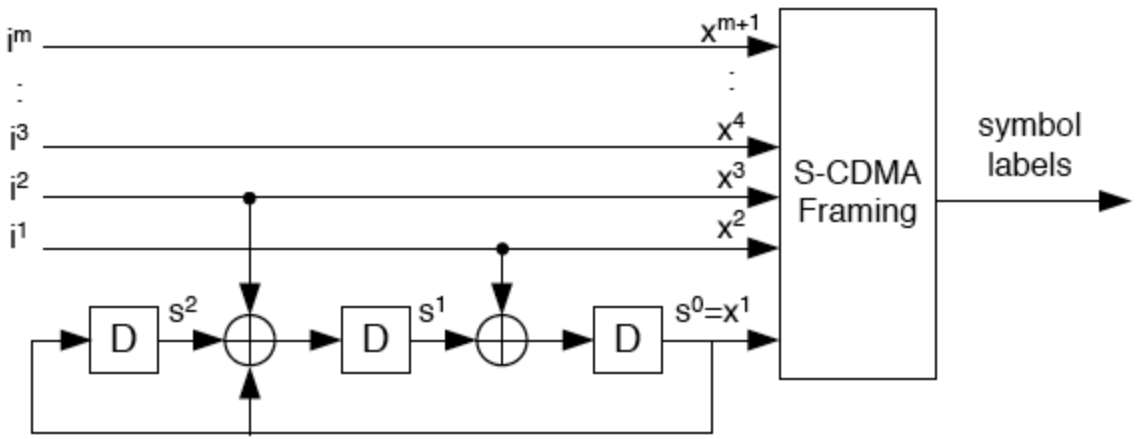
- Modo dinâmico: Os valores de N_r e I_r são calculados dinamicamente bloco a bloco de modo a equalizar a profundidade do entreleçamento.

- No início de cada *burst*, o registo de cifra é re-inicializado com uma semente.
- O velor da semente que é recebido um *Upstream Channel Descriptor* do CMTS.



l

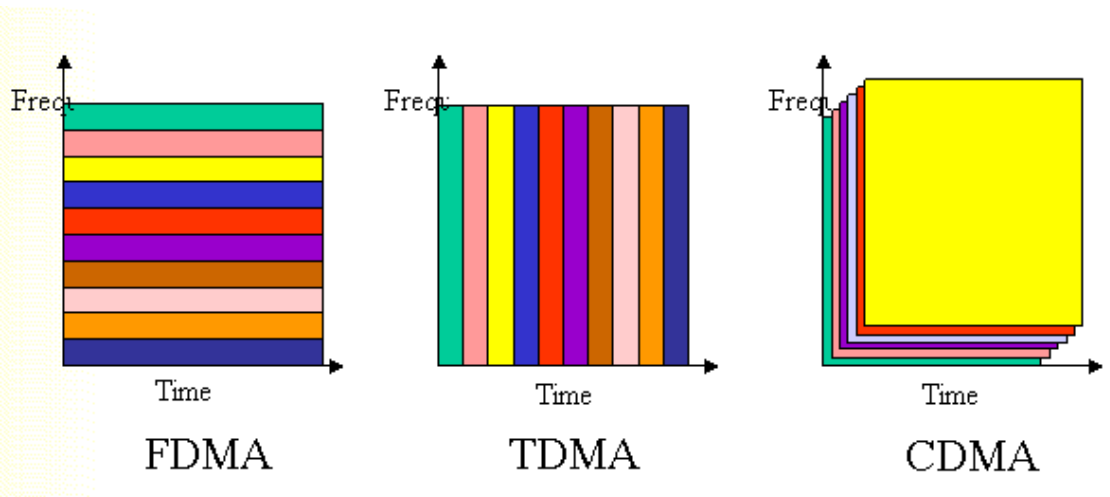
- Em S-CDMA, o suporte de TCM é obrigatório
- Em TDMA, não é normalmente usado TCM
- Suporte obrigatório de m = 1, 2, 3, 4, 5, and 6
  - QPSK0, 8 QAM, 16 QAM, 32 QAM, 64 QAM, and 128 QAM



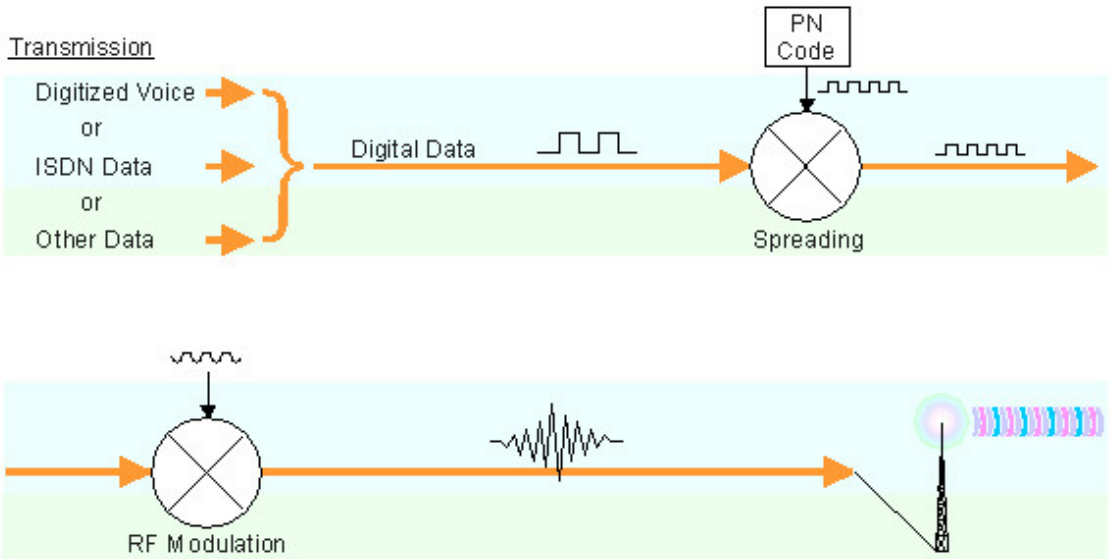
Preâmbulo

- Conjunto de bits introduzidos no início para indicar o começo de uma trama de dados
- Dimensão programável pelo CMTS

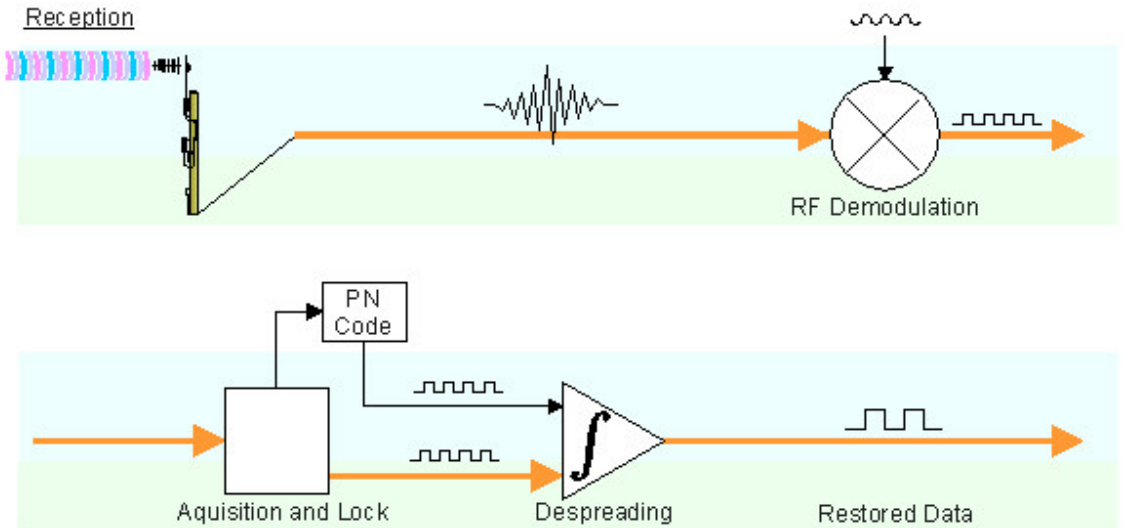
- CDMA
  - Método de partiha do meio baseada em códigos espectrais ortogonais
  - Todos os canais usam as mesmas bandas de frequência e os mesmos slots temporais
  - A distinção entre canais tem lugar pela utilização de códigos ortogonais.
  - Frequente em redes celulares 3G.
- S-CDMA: Combinação de CDMA e TDMA.



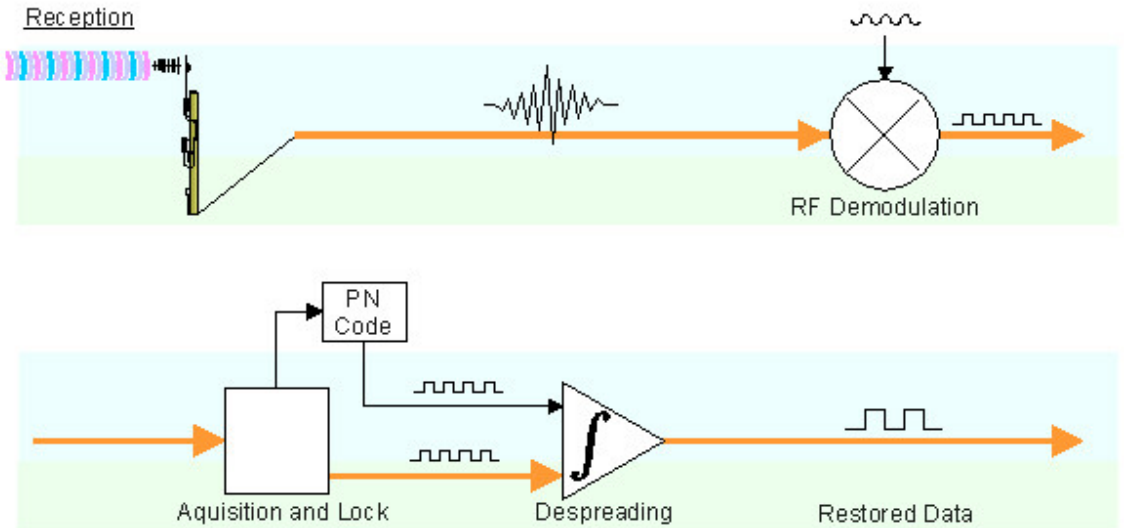
CDMA - transmissor



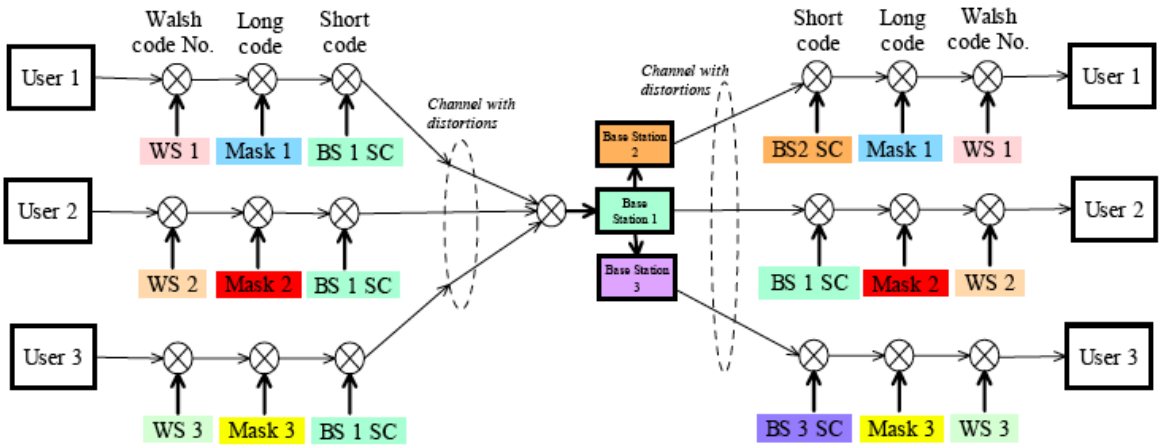
CDMA - receptor



CDMA - receptor



CDMA - multiplexagem

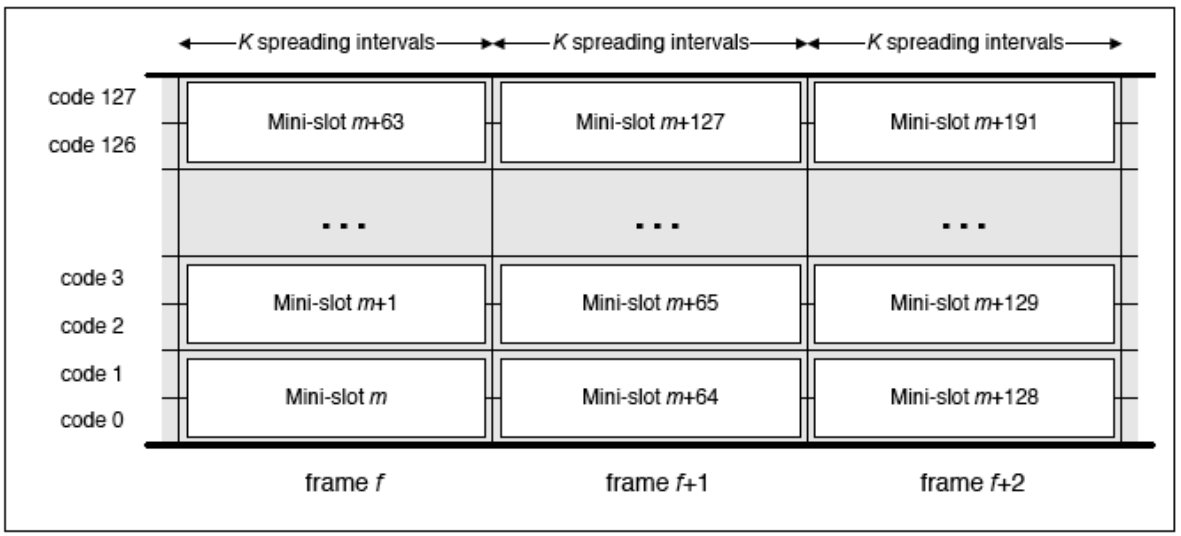


Framer (S-CDMA)

- Responsável pela distribuição dos dados por mini-slots e seu mapeamento por códigos ortogonais de espalhamento espectral.
- Os CM e o CMTS devem ter um protocolo comum sobre a numeração de mini-slots e de como são mapeados.
- A reserva e atribuição é feita pelas mensagens SYNC e UCD (*Upstream Channel Descriptor*)
- Em TDMA a recuperação é feita apenas pelo *time-stamp*.
- Em S-CDMA, é necessário a alocação de códigos e intervalos a cada transmissão

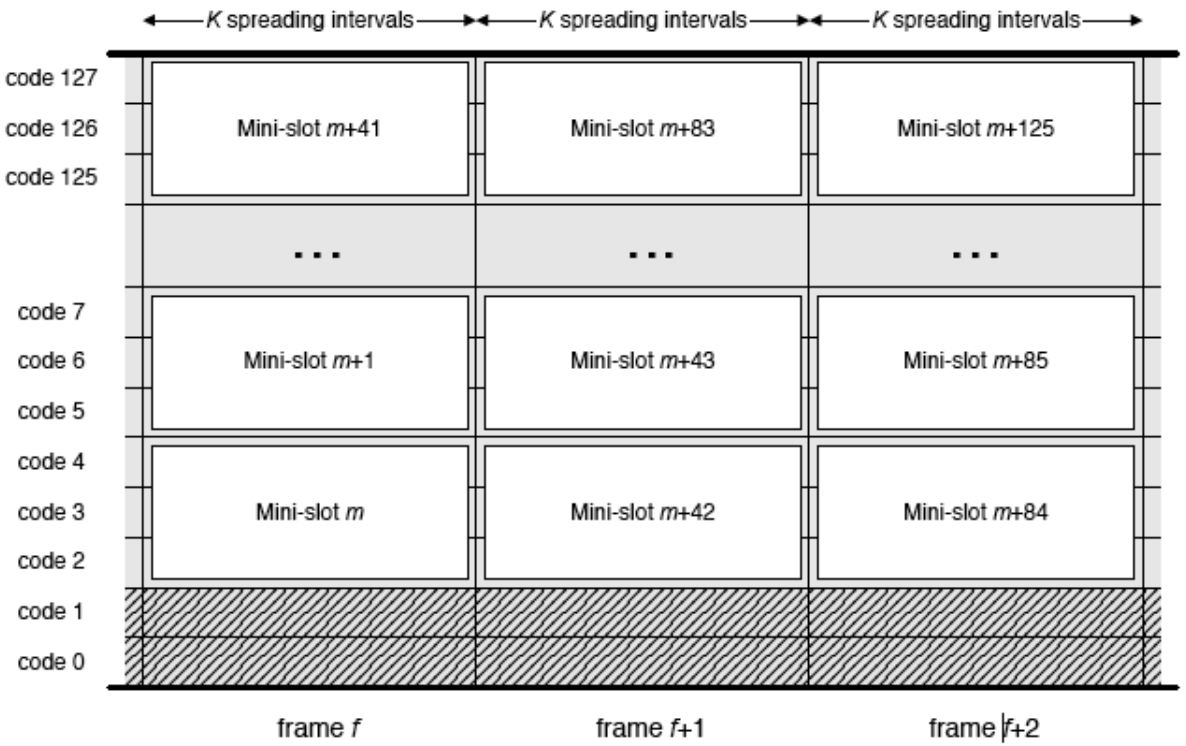
- Cada mini-slot pode ocupar mais do que um código

Exemplo: 2 códigos por mini-slot



Framer (S-CDMA) - numeração dos *mini-slots* (2)

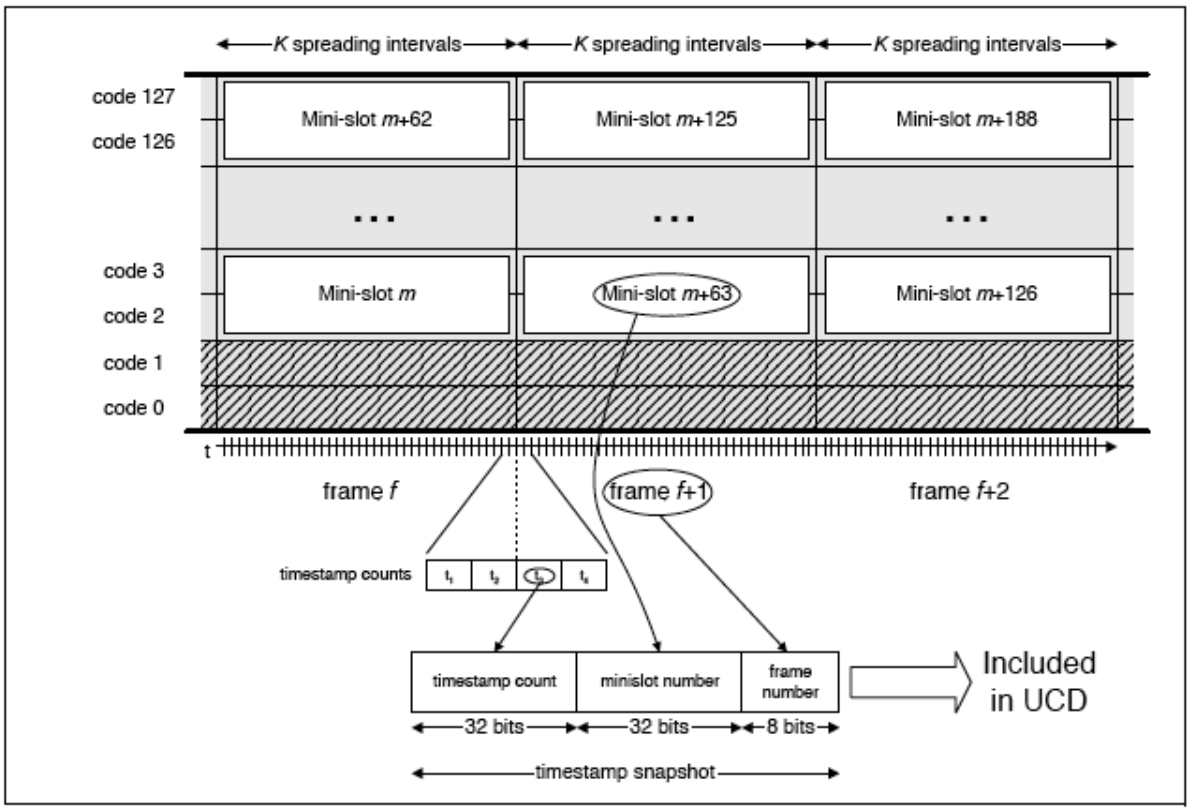
Exemplo: 3 códigos por mini-slot



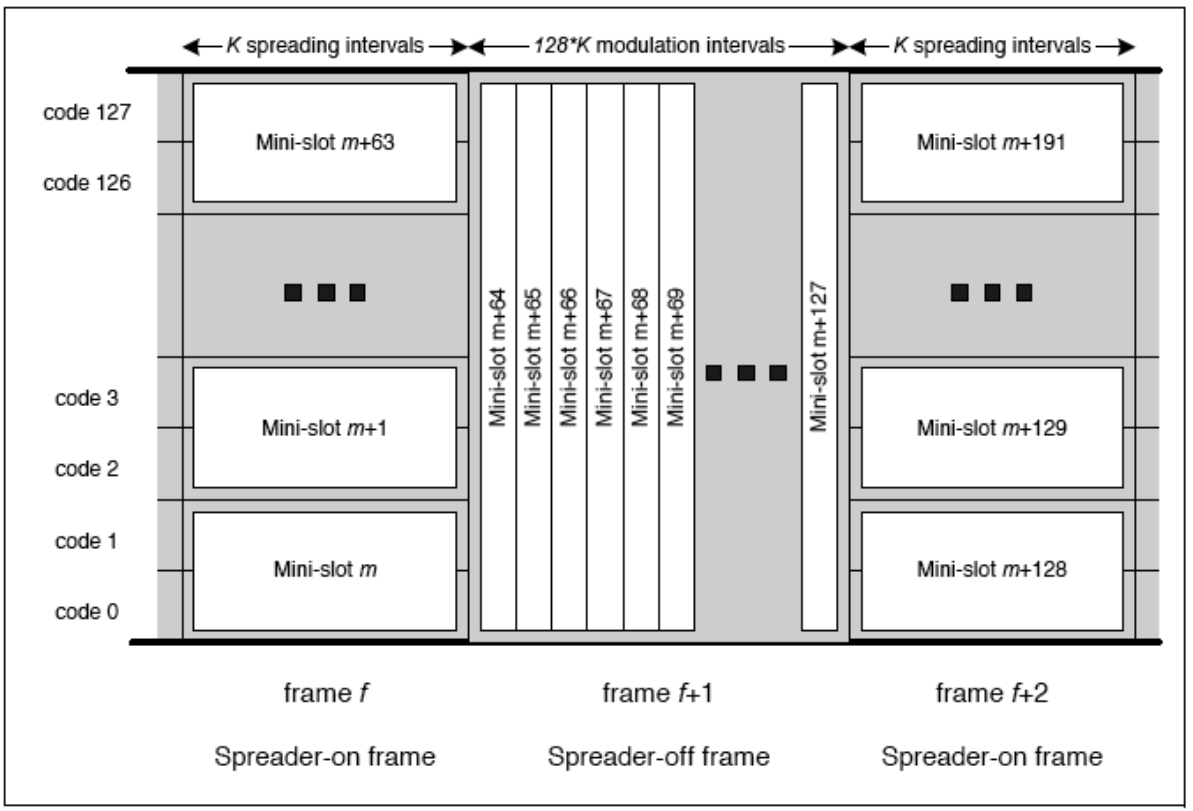
Framer (S-CDMA) - Sincronização

- O funcionamento correcto do sistema exige uma sincronização adequada entre o CMTS e os CMs
- O CMTS envia periodicamente
- Para este efeito, o CMTS e o CM mantêm um contador de mini-slots, um contador de frames e um relógio.
- Antes do envio de cada UCD, o CMTS deve amostrar e identificar, no intervalo de duas frames, o relógio, o número do mini-slot e o número da frame.
- Toda esta informação é incluída na UCD, permitindo a cada CM sincronizar-se periodicamente com o CMTS

Framer (S-CDMA) - Sincronização (2)



- O CMTS deve garantir a existência periódica de frames sem *spreading* para envio de informação ascendente de manutenção.



A camada MAC define

- Largura de banda, controlada pelo CMTS
- *Alocação de minislots* (ascendente)
- Optimização dinâmica de conteção e reserva de recursos (ascendente)
- Eficiência da largura de banda
- Extensões para suporte ATM e outras PDUs
- Qualidade de serviço
  - Garantia de largura de banda e latência
  - Classificação de pacotes
- Segurança
- Suporte de vários ritmos de transmissão

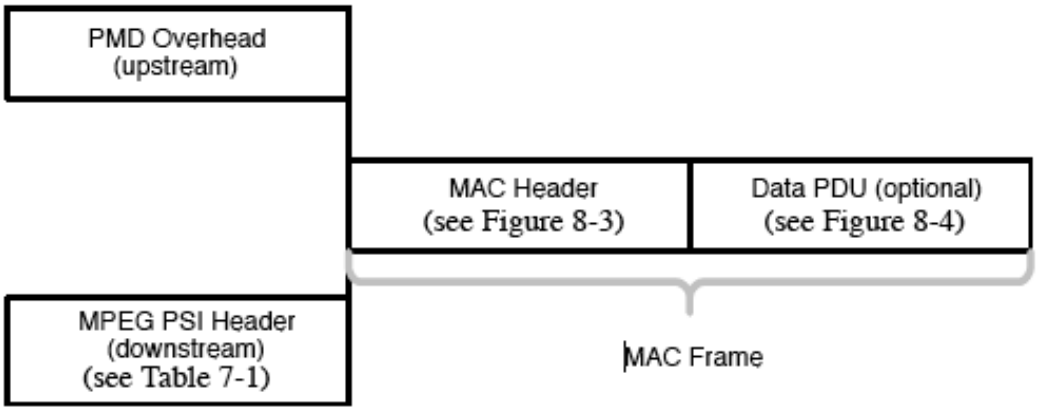
Organização

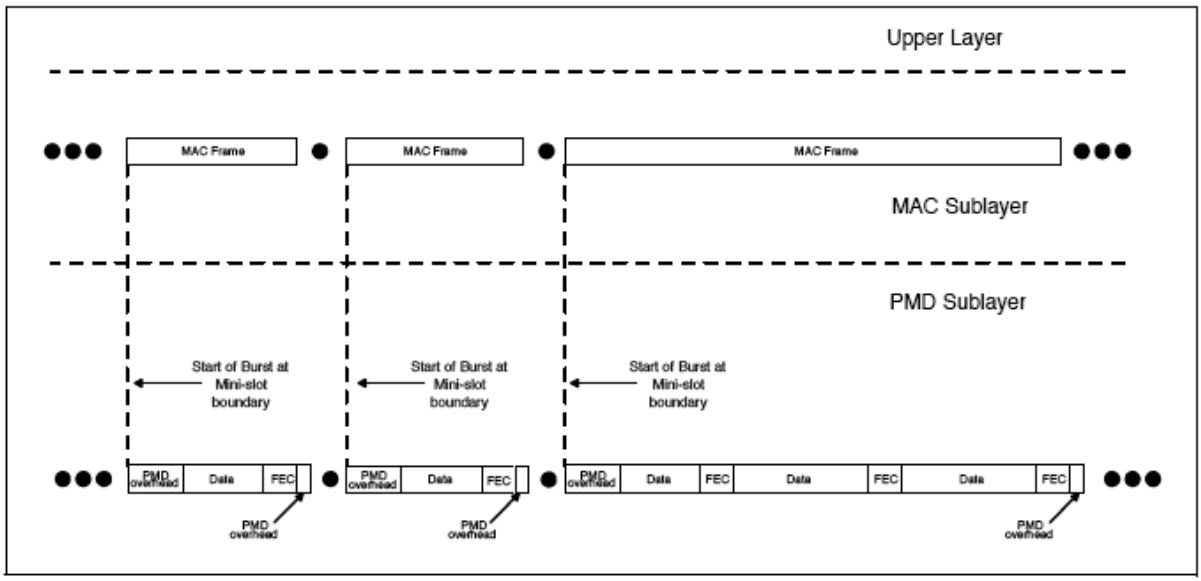
- Cada CMTS deve servir os streams ascendentes e descedente de todos os CMs associados.
- Cada CM acede a uim canal descedente ou ascedente
  - O CM deve descartar todos os pacotes cujo endereço que não correspondam ao seu endereço MAC.
  - O CMTS deve descartar todos os pacotes de origem que não sejam unicast.
- Um domínio da subcamada MAC é uma colecção de canais ascendentes e descedentes sobre o qual opera um único protocolo de gestão e reserva de recursos MAC. Normalmente, tem associado um CMTS e um conjunto de CMs.
- MSAP - MAC Service Access Point
  - Associado a um domínio da subcamada MAC
- *Service Flows*
  - Mecanismo que a gestão de de QoS ascendente e descedente
  - Parte integrante do sistema de reserva de largura de banda
  - Cada CM deve suportar pelo menos dois service flows (um ascedente e um descendente)
  - Modems mais complexos poderão suportar multi-serviços.

- Mini-slot: de granularidade para oportunidades de transmissão ascendentes
- Uma PDU pode ocupar mais do que um mini-slot
- Modo TDMA
  - Mini-slot: múltiplo de 6,25μs, em potências de 2: $(1, 2, 4, ..., 128) \times 6,25\mu s$
- Modo S-CDMA
  - Apenas dependente da configuração definida na UCD

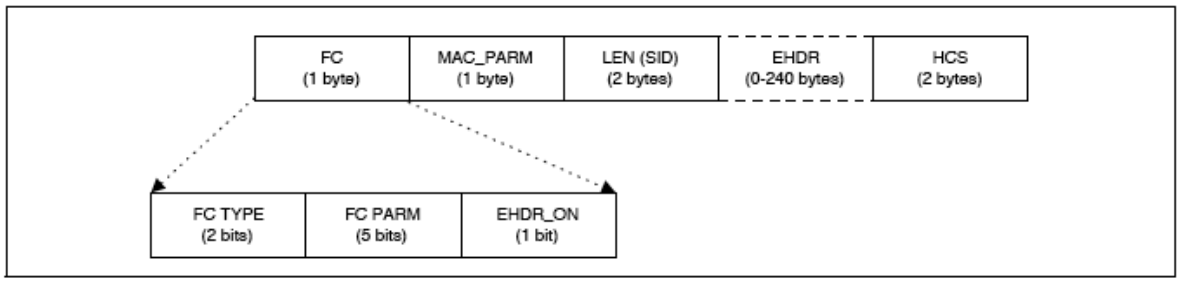
Trama MAC

- Uma trama MAC é a unidade básica de transferência entre o CMTS e os modems.
- É utilizada a mesma estrutura na direcção ascendente e descendente




Upper Layer
MAC Frame
MAC Frame
MAC Frame
MAC Sublayer
PMD Sublayer
Start of Burst at Mini-slot boundary
Start of Burst at Mini-slot boundary
Start of Burst at Mini-slot boundary
PMD overhead
Data
FEC
PMD overhead
Data
FEC
PMD overhead
Data
FEC
Data
FEC
Data
FEC
PMD overhead
PMD overhead
PMD overhead

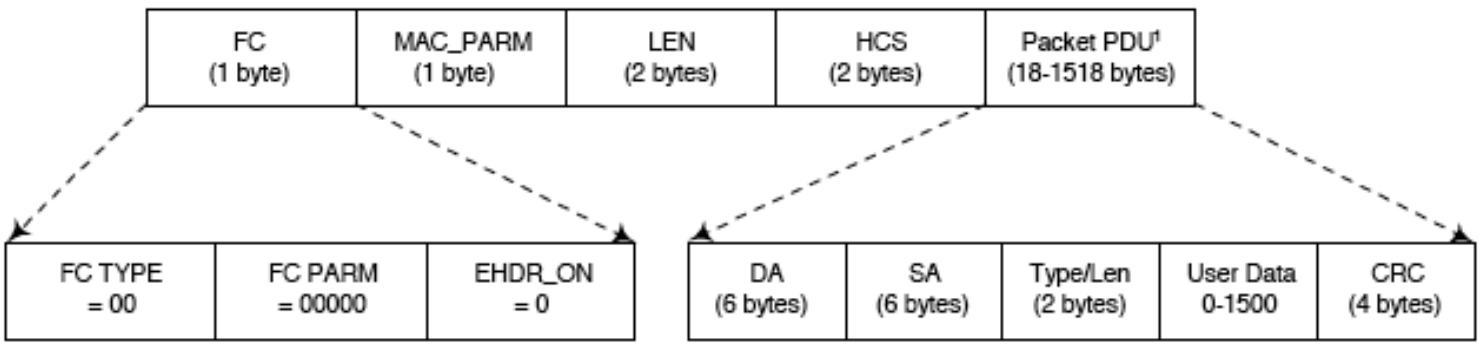
Cabeçalho da trama MAC



- FC-type: indentifica o tipo de PDU
- FC_PARM: parâmetro dependente do FC-Type: pode especificar o comprimento do campo EDHR ou em caso de concatenação de tramas, contador de tramas
- EHDR_ON: presença de EHDR
- LEN Comprimento da trama (6 bytes + EHDR)
- EHDR Extended MAC header; variable size
- HCS Mac Header Check sequence

PDU

- A camada MAC pode transportar vários tipos de PDU de camadas superiores.
  - Ethernet/802.3, ATM e outras
- Na especificação do DOCSIS 2.0, apenas a trama Ethernet/802.3 é especificada
- FC_TYPE=00, FC_PARM=0000

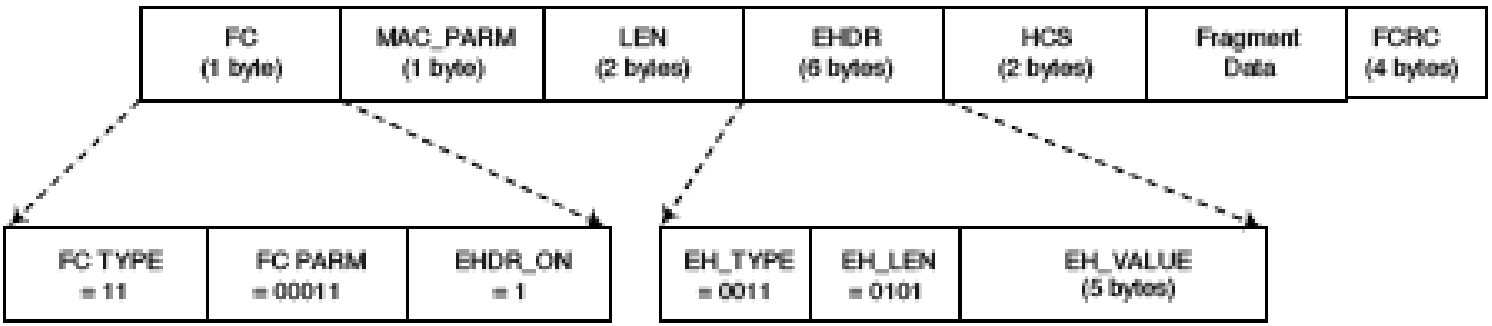


Tipos de cabeçalhos MAC

- Há vários cabeçalhos MAC que podem ser usados em casos muito específicos, tal como reajuste de potências de transmissão, reajuste de largura de banda disponível e fragmentação e concatenação de várias tramas MAC.
- FC_TYPE=11
- Tipo específico definido por FC_PARM
  - 00000 Cabeçalho de temporização
  - 00001 Cabeçalho MAC de gestão
  - 00010 Cabeçalho de pedidos
  - 00011 Cabeçalho de fragmentação
  - 11100 Cabeçalho de concatenação

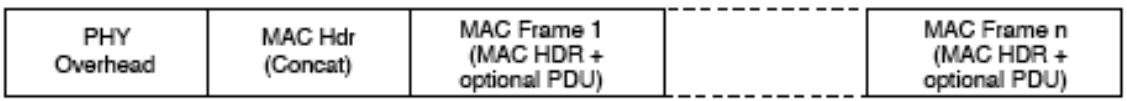
- Temporização
  - Sentido descendente: transmite o Tempo de Referência Global para sincronização
  - Sentido ascendente: temporização e ajuste de potência.
- Gestão
  - Suporte de mensagens de gestão
- Pedidos
  - Pedidos de largura de banda

- Fragmentação:
  - Só usada no sentido ascedente
  - Implementa o mecanismo necessário à fragmentação tramas MAC de dimensão elevada.

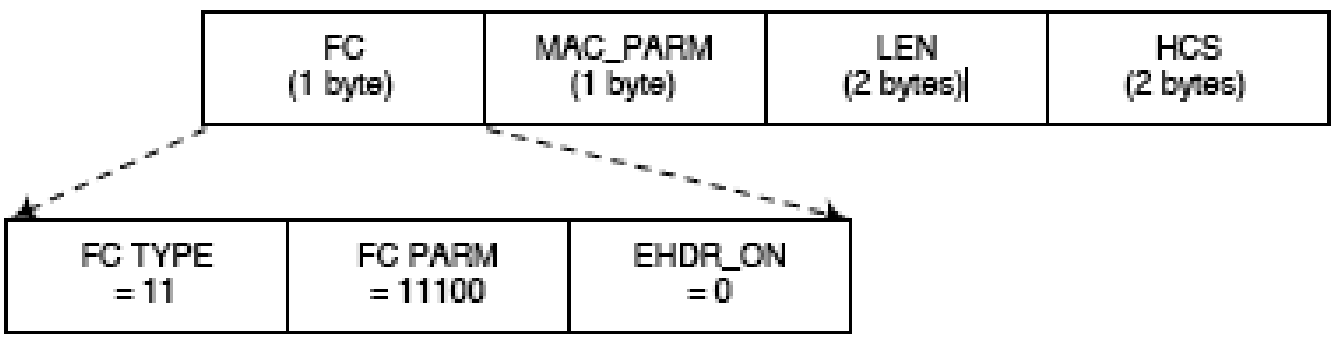


- No caso de tramas de fragmentação, o campo EH_VALUE inclui, entre outra informação, 4 bits para a numeração dos fragmentos que permite a sua reconstrução no CMTS.

- Concatenação
  - Permite que múltiplas tramas MAC sejam enviadas num único *burst*.



  - Cada *burst* só pode incluir um cabeçalho de concatenação

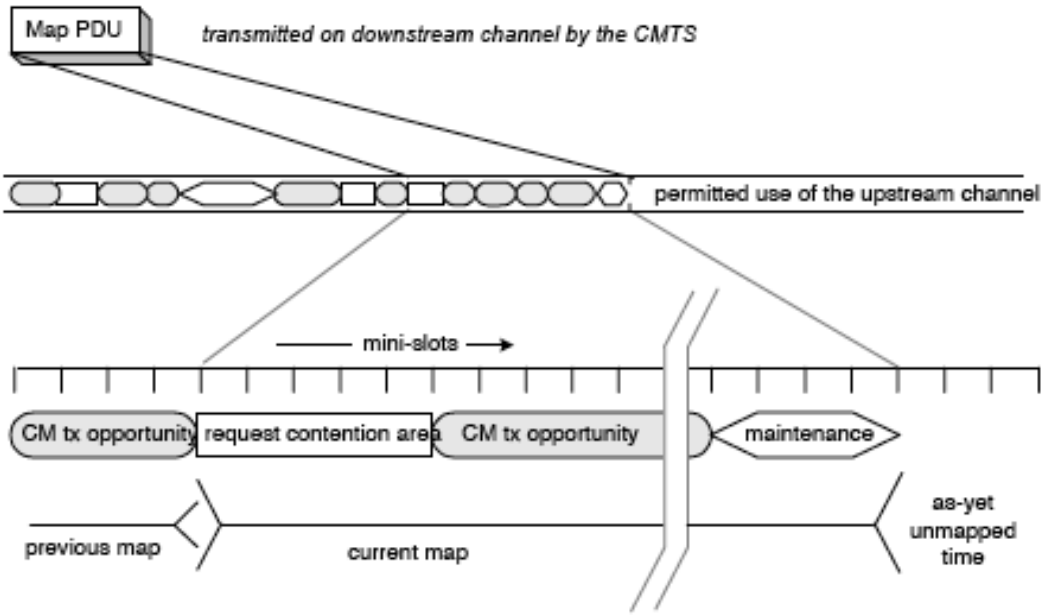


  - Este inclui informação sobre:
    * O número de tramas concatenadas,
    * O comprimento total de todas as tramas
    * Não é permitida concatenação hierárquica

Atribuição de banda ascendente

- O canal de dados ascendente é modelado como um *stream* de mini-slots
- O CMTS é responsável por
  - Gerar a referência temporal para sincronização dos CMs
  - Controlar o acesso aos mini-slots por parte dos CMs
    - O acesso aos mini-slots é controlado por um protocolo que estabelece as regras de pedido, atribuição e utilização da largura de banda ascedente.
- A norma DOCSYS não define o algoritmo de atribuição de largura de banda pelo CMTS, que pode ser dependente do fabricante. Apenas estabelece o protocolo usado com os CMs para distribuir esta informação.
- A atribuição de largura de banda é realizada pelo envio de uma mensagem MAC de gestão designada *allocation MAP* no canal descendente que descreve a utilização de mini-slots no canal ascendente.

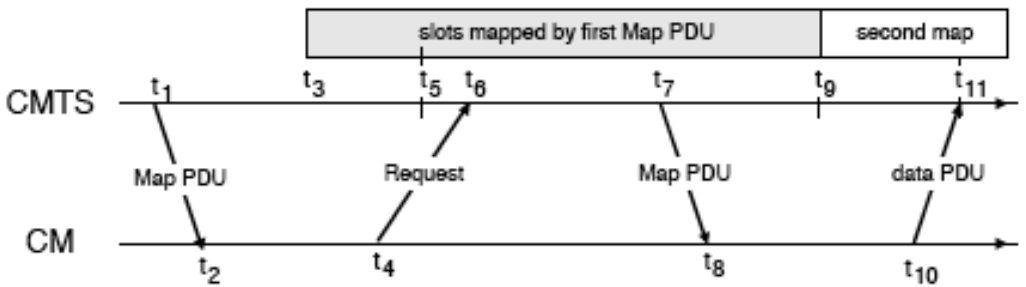
Atriibuição do canal ascendente



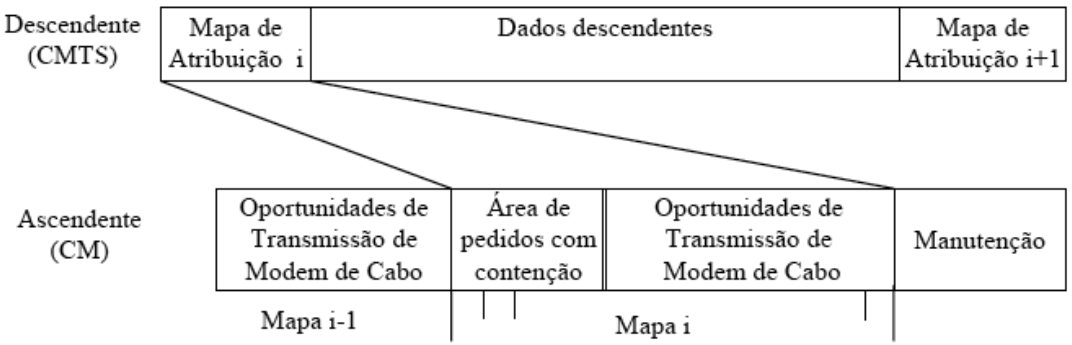
Elementos básicos da reserva de banda

- Cada CM tem um ou mais indentificadores de serviço (SIDs) de 14 bits, para além do endereço de 48bits (MAC).
- Os mini-slots encontram-se numerados relativamente a um referência definida pelo CMTS. Esta referência é distribuída por meio de pacotes de sincronização
- Os CMS podem realizar pedidos de reserva de largura de banda
- O allocation map não pode atribuit mais do que 4096 minislots de cada vez.

Protocolo de reserva e atribuição de largura de banda



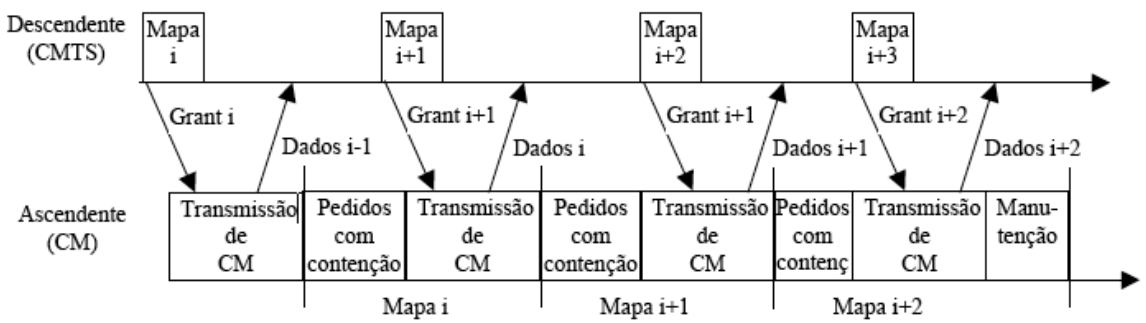
Formato das mensagens



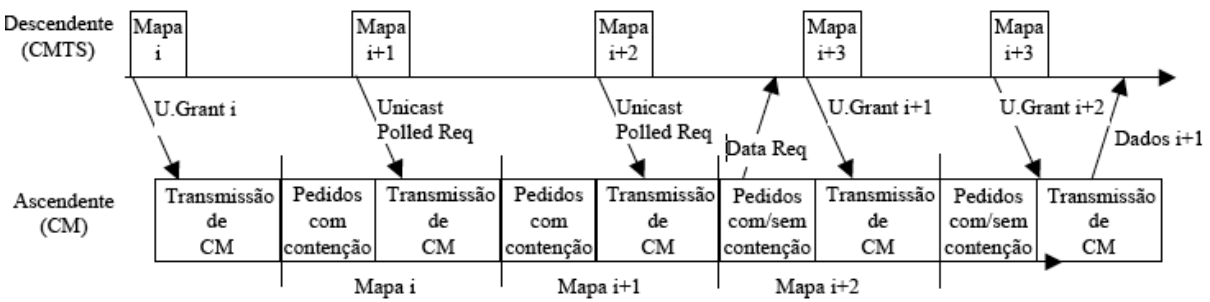
- DOCSIS 2.0 fornece diversos serviços upstream baseados em *Service Flows* e em listas de parâmetros de QoS associados a cada serviço.
- Cada serviço é ajustado a um tipo específico de fluxo de dados.
- Serviços básicos:
  - Unsolicited Grant Service (UGS) - Serviços de tempo real que gerem pacotes de comprimento fixo (ex. VoIP);
  - Unsolicited Grant Service with Activity Detection (UGS-AD) - Suporte de fluxos UGS com períodos de inactividade (ex. VoIP com supressão de silêncio);
  - Real-Time Polling Service (rtPS) - Serviços de tempo real que gerem pacotes de dados de comprimento variável (ex. MPEG);
  - Non-Real-Time Polling Service (nrtPS) - para suportar serviços que não sejam de tempo real que requeiram dados de tamanho variável;
  - Best Effort (BE) service - tráfego BE.

UGS - Unsolicited Grant Service

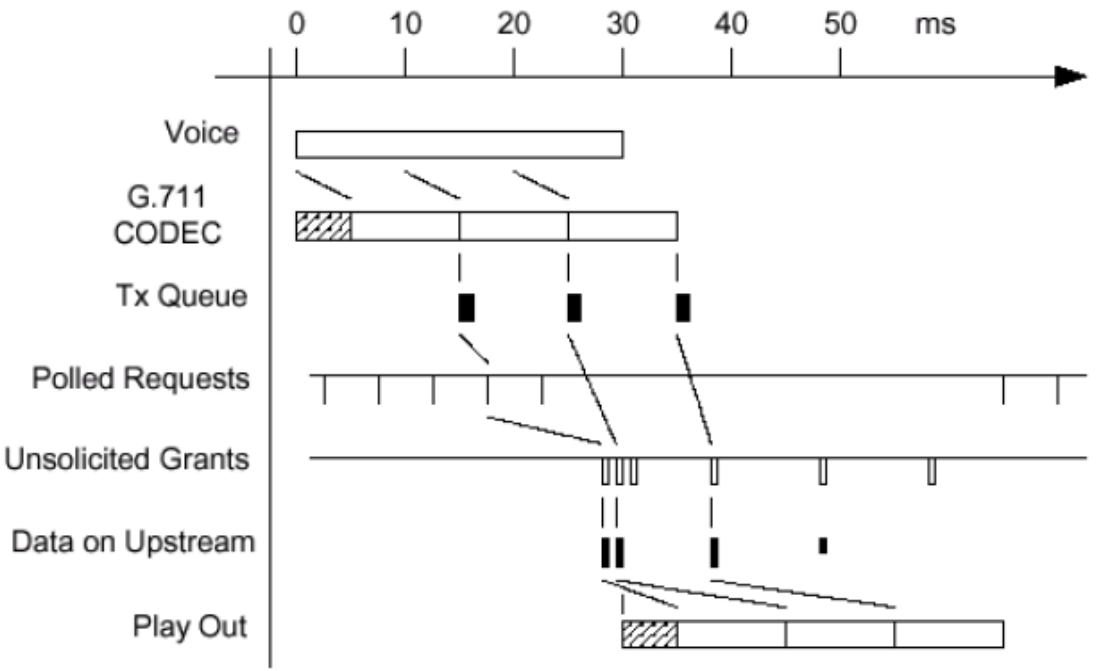
- Parâmetros de configuração do serviço:
  - Nominal Grant Interval
  - Unsolicited Grant Size
  - Tolerated Grant Jitter
  - Grants per Interval
- Nominal Grant Interval é escolhido de modo a igualar o intervalo entre pacotes.
  - Ex: VoIP com periodicidade de 20ms: Nominal Grant Interval = 20 ms.



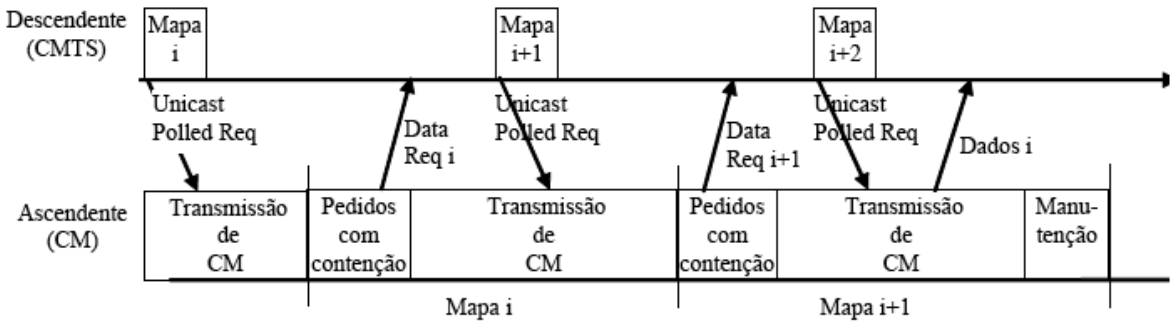
- O Headend utiliza um algoritmo de detecção de actividade para examinar o estado do fluxo.
- Quando um fluxo muda do estado activo para o estado inactivo passa a ser usado um polling periódico.



- Voice Activity Detection



- O CMTS gera oportunidades periódicas de polling



Outros fluxos

- nrtPS - Non-real-time polling requests
- Best effort

Baseline Privacy Plus (BPI+)

- Objectivo: privacidade de dados sobre a rede de cabo.
  - Usado um sistema de PKI com as chaves geridas e distribuídas centralmente pelo CMTS
- Princípio protocolo de manuseamento de chave de autenticação entre cliente e servidor
- Distribuição da chave controlada pelo CMTS
  - Nota: as especificações iniciais BPI foram substituídas pelo BPI+ dado que na versão original o CM não era autenticado.
- Compreeende dois protocolos:
  - Protocolo de encapsulamento e encriptação
  - Protocolo de manuseamento de chaves
- BPI+ cifra apenas o payload de dados do pacote MAC, mas não o cabeçalho.
- Algoritmos: modo Cipher Block Chaining (CBC) do algoritmo US Data Encryption Standard (DES)